CLAIMS

1. A method of establishing trust between independent first and second computer-type entities, the first entity operating in a trusted manner on a computing device and seeking a trust-based relationship with the second entity, whereby the first entity constructs an attestation message to be delivered to the second entity, the attestation message including a code identifier (code ID) representative of the first entity and data relevant to the purpose of the trust-based relationship, the second entity having knowledge of each valid code ID corresponding to the first entity, the first entity appends a digital signature to the attestation message and a certificate chain leading back to a trusted root authority, the signature being based on the code ID and data thereof and being verifiable based on a security key included in the certificate chain, the certificate chain including at least one certificate therein proffering trustworthiness of the computing device of the first entity, and the first entity sends the attestation message to the second entity and the second entity receives same, the method comprising:

the second entity verifying the signature of the received attestation message based on the included security key, whereby alteration of the code ID or data of the attestation message should cause the signature to fail to verify, the second entity based on such a failure dishonoring such attestation message;

the second entity deciding whether to in fact enter into the trust-based relationship with the first entity based on the code ID and the data in the attestation message;

the second entity upon deciding to in fact enter into the trust-based relationship with the first entity constructing a trust message to be delivered to the first entity, the trust message establishing the trust-based relationship and including therein a secret to be shared between the first and second entities,

where such shared secret allows such first and second entities to communicate in a secure manner; and

the second entity sending the trust message to the first entity and the first entity receiving same, whereby the first entity obtains the shared secret in the trust message and employs the shared secret to exchange information with the second entity according to the established trust-based relationship with such second entity.

2. The method of claim 1 wherein the first entity encrypts at least one of the code ID and the data of the attestation message according to a key available to the second entity, the method further comprising the second entity decrypting such encrypted matter.

3. The method of claim 1 wherein the second entity consumes the attestation message by application of same to a verifying function that automatically verifies the attestation message based on a format thereof and that extracts relevant information from such verified attestation message for use by the second entity.

4. The method of claim 1 wherein the second entity decides based on the code ID of the first entity in the attestation message therefrom whether the second entity can be trusted, and also decide based on the certificate chain of the message whether the computing device can be trusted.

5. The method of claim 4 wherein the second entity identifies the first entity based on the code ID thereof and decides based on the identity of the first entity whether such first entity can be trusted

6. The method of claim 5 wherein the second entity determines that the identified first entity is not on a do-not-trust list.

7. The method of claim 4 wherein the second entity determines that the code ID is a known code ID and that the first entity can be trusted based on such code ID.

8. The method of claim 4 wherein the second entity determines from the certificate chain whether the computing device of the first entity should be trusted to instantiate and execute the first entity in a trusted manner and should be trusted to calculate the code ID properly.

9. The method of claim 8 wherein the second entity determines that each certificate in the certificate chain is not on a do-not-trust list.

10. The method of claim 1 wherein the second entity constructs a trust message including therein a shared secret comprising a symmetric key (K) that the first and second entities shall each employ to encrypt and decrypt messages therebetween.

11. The method of claim 10 wherein the second entity constructs a trust message including therein the symmetric key (K) encrypted according to a public key of the first entity (PU-1) to result in (PU-1(K)), the second entity obtaining (PU-1) from the certificate chain of the attestation message, and wherein the first entity obtains the symmetric key (K) from the received trust message by applying a private key (PR-1) corresponding to (PU-1) to (PU-1(K)) to result in (K).

12. The method of claim 1 wherein the second entity constructs a trust message further including therein an identification of a cryptographic algorithm to be employed in connection with the shared secret.

13. The method of claim 1 wherein the second entity constructs a trust message further including therein the code ID of the first entity as obtained from the attestation message.

14. The method of claim 1 wherein the second entity constructs a trust message further including relevant trust data encrypted according to a key available to the first entity, and wherein the first entity decrypts the encrypted trust data by applying the key thereto.

15. The method of claim 1 wherein the second entity constructs a trust message further including an expiration time after which the shared secret and the established trust-based relationship are no longer valid.

16. The method of claim 1 wherein the second entity creates the trust message by application of the shared secret and other relevant information to a sealing function that automatically produces the trust message in an appropriate format that is accessible to the first entity.

17. The method of claim 1 whereby the trust message is a first trust message and the shared secret is a first shared secret, the method further comprising:

the second entity constructing a second trust message to be delivered to the first entity, the second trust message including therein a second secret to be shared between the first and second entities, where such second shared secret allows such first and second entities to communicate in a secure manner;

the second entity sending the second trust message to the first entity and the first entity receiving same, whereby the first entity obtains the second shared secret in the trust message and employs the second shared secret to exchange information with the second entity, the first shared secret no longer being valid.

18. The method of claim 1 wherein prior to the first entity constructing the attestation message, the first entity sends a can-attest message

to the second entity, the can-attest message stating that the first entity can send an attestation message but that the first entity would like to know from the second entity whether such an attestation message is required by such second entity and if so any requirements that such second entity has with regard to such attestation message, the method further comprising the second entity sending an attestation-wanted message to the first entity in response to the can-attest message, the attestation-wanted message stating that the second entity does in fact require an attestation message from the first entity and that the attestation message as sent by the first entity must adhere to certain requirements as defined in such attestation-wanted message, whereby the first entity thereafter sends the attestation message in accordance with the requirements stated in the attestation-wanted message.

19. A method of establishing trust between independent first and second computer-type entities, the first entity operating in a trusted manner on a computing device and seeking a trust-based relationship with the second entity, the method comprising:

the first entity constructing an attestation message to be delivered to the second entity, the attestation message including a code identifier (code ID) representative of the first entity and data relevant to the purpose of the trust-based relationship, the second entity having knowledge of each valid code ID corresponding to the first entity;

the first entity appending a digital signature to the attestation message and a certificate chain leading back to a trusted root authority, the signature being based on the code ID and data thereof and being verifiable based on a security key included in the certificate chain, the certificate chain including at least one certificate therein proffering trustworthiness of the computing device of the first entity;

the first entity sending the attestation message to the second entity and the second entity receiving same, whereby the second entity verifies the signature of the received attestation message based on the included security key,

whereby alteration of the code ID or data of the attestation message should cause the signature to fail to verify, the second entity based on such a failure dishonoring such attestation message, the second entity decides whether to in fact enter into the trust-based relationship with the first entity based on the code ID and the data in the attestation message, the second entity upon deciding to in fact enter into the trust-based relationship with the first entity constructs a trust message to be delivered to the first entity, the trust message establishing the trust-based relationship and including therein a secret to be shared between the first and second entities, where such shared secret allows such first and second entities to communicate in a secure manner, and the second entity sends the trust message to the first entity and the first entity receiving same; and

the first entity obtaining the shared secret in the trust message and employing the shared secret to exchange information with the second entity according to the established trust-based relationship with such second entity.

20. The method of claim 19 wherein the first entity constructs an attestation message including a code identifier (code ID) calculated from a digest of the first entity, whereby alteration of the first entity causes the code ID to change.

21. The method of claim 20 wherein the first entity constructs an attestation message including a code identifier (code ID) calculated from a digest of the first entity and from security information relating thereto, whereby alteration of the first entity or the security information causes the code ID to change.

22. The method of claim 19 wherein the first entity constructs an attestation message including trust information relevant to the trust-based relationship.

23. The method of claim 19 further comprising a code ID calculator on the computing device of the first entity calculating the code ID, the code ID calculator operating in a trusted manner on the computing device.

24. The method of claim 19 further comprising the first entity encrypting at least one of the code ID and the data of the attestation message according to a key available to the second entity, and the second entity decrypting such encrypted matter.

25. The method of claim 19 wherein the first entity creates the attestation message by application of the code ID and data thereof to a quoting function that automatically produces the attestation message in an appropriate format that is accessible to the second entity.

26. The method of claim 19 wherein the second entity constructs a trust message including therein a shared secret comprising a symmetric key (K) that the first and second entities shall each employ to encrypt and decrypt messages therebetween, the symmetric key (K) being encrypted according to a public key of the first entity (PU-1) to result in (PU-1(K)), the second entity obtaining (PU-1) from the certificate chain of the attestation message, the method comprising the first entity obtaining the symmetric key (K) from the received trust message by applying a private key (PR-1) corresponding to (PU-1) to (PU-1(K)) to result in (K).

27. The method of claim 19 wherein the second entity constructs a trust message further including relevant trust data encrypted according to a key available to the first entity, the method comprising the first entity decrypting the encrypted trust data by applying the key thereto.

28. The method of claim 19 wherein the first entity consumes the trust message by application of same to an unsealing function that automatically

extracts the shared secret and other relevant information from such trust attestation message for use by the first entity.

29. The method of claim 19 whereby the trust message is a first trust message and the shared secret is a first shared secret, and whereby the second entity constructs a second trust message to be delivered to the first entity, the second trust message including therein a second secret to be shared between the first and second entities, where such second shared secret allows such first and second entities to communicate in a secure manner, and the second entity sends the second trust message to the first entity and the first entity receives same, the method further comprising the first entity obtaining the second shared secret in the trust message and employing the second shared secret to exchange information with the second entity, whereby the first shared secret is no longer valid.

30. The method of claim 19 further comprising, prior to the first entity constructing the attestation message, the first entity sending a can-attest message to the second entity, the can-attest message stating that the first entity can send an attestation message but that the first entity would like to know from the second entity whether such an attestation message is required by such second entity and if so any requirements that such second entity has with regard to such attestation message, whereby the second entity sends an attestation-wanted message to the first entity in response to the can-attest message, the attestation-wanted message stating that the second entity does in fact require an attestation message from the first entity and that the attestation message as sent by the first entity must adhere to certain requirements as defined in such attestation-wanted message, the first entity thereafter sending the attestation message in accordance with the requirements stated in the attestation-wanted message.